Digital Workplace Services

Managed End User Device Services – Service Description

This Service Description ("**Managed End User Device Services – Service Description**") contains the terms governing the provision of **Managed End User Device Services** by Interactive Pty Ltd ABN 17 088 952 023 of 461 Williamstown Road, Port Melbourne VIC 3207 ("**Interactive**") to the customer named in the CMS SOW ("**Customer**") that applies to this Managed End User Device Services – Service Description.

This Managed End User Device Services – Service Description forms part of the Agreement, also containing the Digital Workplace Services – Service Terms found at www.interactive.com.au/terms-and-conditions and the Master Services Agreement.

1. Managed End User Device Services

1.1 Interactive will provide the Managed End User Device Services to the Customer for the support and management of the Customers in scope Devices.

1.2 The Managed End User Device Services consists of the following, each as further described in the relevant Service Specification contained in this Service Description:

(a) Application Packaging

(b) Software Distribution

(c) Remote Desktop Support

(d) Patch Management

(e) Device Security Management

(f) Managed Operating Environment ("MOE") Management

(g) Device Lifecycle Management

(h) Reporting

1.3 If set out in the CMS SOW, Interactive will provide the following optional Managed End User Device Services, each as further described in this Service Description:

(a) Onsite Desktop Support

(b) Managed Mobility Services

1.4 Interactive will only use personnel with suitable experience and certifications to perform the Managed End User Device Services and will perform the Managed End User Device Services with due care and skill and in a professional and workmanlike manner.

1.5 Interactive will comply with the Customer's reasonable physical security and access policies, which have been provided to Interactive in advance, while performing Managed End User Device Services at an Onsite Location.

1.6 Interactive relies on the information provided to it by the Customer to be able to perform the Managed End User Device Services.

1.7 The Customer acknowledges that any Service Level Targets set out in the Service Terms and this Service Description are only targets, and that Interactive's failure to meet any Service Level Target is not a breach of the Agreement.

1.8 The Customer may request up to 2 IMACs per month. Any additional IMACs requested in a month will be charged at the IMAC Support Fee set out in the CMS SOW. Unused requests for IMACs do not rollover.

1.9 Any single IMAC request that contains a request for multiple requests within it (e.g., one request asking for onboarding of multiple Users) will be treated as individual requests for the purposes of calculating the monthly Service Fee (e.g., if one request is lodged to onboard 20 Users, then this would count as 20 Service Calls and the relevant charges would apply.

1.10 Interactive will provide access to the Customer Portal for Users to lodge requests into Interactive's ITSM platform. No other access to or functions within the ITSM platform will be provided to the Customer.

2. General Terms

2.1 Interactive will onboard the Customer's Devices into the Managed End User Device Services environment.

2.2 The Customer's liability to pay the monthly Service Fees for the Managed End User Device Services commences from the Service Start Date, even if transition services are included but not completed.

2.3 To the extent required by law, the Customer shall notify the Users of the Managed End User Device Services that their data may be processed for the purpose of disclosing it to law enforcement or other governmental authorities as directed by Interactive. The Customer shall obtain the Users' consent to the same.

2.4 The Customer is responsible for maintaining the currency (including renewal and cancellation) of its existing subscriptions or licenses that are provided by third parties.

2.5 Interactive will place an order for any dependent/ third-party licenses required to deliver the Managed End User Device Services detailed in the CMS SOW and charge it to the Customer.

3. Term of Managed End User Device Services

3.1 Interactive will provide the Managed End User Device Services for the Individual Term. The Individual Term commences on the Service Start Date (being the date notified by Interactive in accordance with clause 5.1(b).

3.2 For planning and pricing and ensuring continuity of service purposes, and unless otherwise detailed in the CMS SOW or otherwise agreed in writing:

(a) not less than 60 days before the end of the Service Term or a current Further Term of a Statement of Work, Interactive shall send a written notice to the Customer reminding them of the upcoming renewal;

(b) not less than 30 days before the end of the Service Term or a current Further Term of a Statement of Work either party may serve written notice on the other party stating it will not renew the Statement of Work; and

(c) if no such notice is served under clause 3.2(b), each Statement of Work renews for successive terms of the lesser of (i) the original contract term; or (ii) 12 months (each successive term being a "Further Term"), at the end of its Service Term and each Further Term.

4. General Customer Obligations

4.1 The Customer must ensure that all Devices meet the following criteria:

(a) permit the installation of software monitoring and management agents.

(b) administration login is restricted to authorised Interactive personnel.

(c) Users do not have any administration rights on the Devices.

4.2 The Customer shall provide Interactive with the Device inventory information reasonably required to enable Interactive to perform the Managed End User Device Services, including but not limited to: Device make, model, age, location, User assigned, warranty status and hardware support status.

4.3 The Customer must advise Interactive if any Device inventory information Changes, including:

(a) advance notice of any Changes to Remote Locations or Onsite Locations; and

(b) significant Changes to quantity of Service Calls or Devices.

4.4 The Customer shall provide Interactive with:

(a) physical access to the Onsite Location (where applicable); and

(b) access to the Customer's network and the IT Environment, which may be physical or by VPN connectivity as required by Interactive.

4.5 The Customer is responsible to protect and backup its own data and equipment including on the Devices.

4.6 If the Customer creates new accounts for Interactive to use while performing the Managed End User Device Services, the Customer shall ensure that the accounts are set up to enable Interactive to perform the Managed End User Device Services (for example, the account must have the appropriate security and access credentials). The Customer must delete any such accounts on termination of the CMS SOW.

4.7 The Customer must:

(a) Provide Interactive with at least 30 days' notice of the exit date of the incumbent provider and coordinate with the incumbent provider of any knowledge transfer as applicable.

(b) Ensure that appropriate communications networks are in place to enable Interactive to provide the Managed End User Device Services.

(c) Provide personnel contact details for each Onsite Location and Remote Location as required.

(d) Provide Interactive personnel and representatives site access as required.

(e) Provide all passwords for the administration logins for the Devices and ensuring that Users do not have administration logins for the Devices.

(f) Ensure that hardware and software maintenance and support coverage is maintained on all Devices.

(g) Ensure the hardware and software (including operating system) is supportable to vendor specifications and remains supportable for the Individual Term.

(h) Pay any costs incurred in connection with upgrades to hardware and software as may be required to maintain vendor currency.

(i) Log all Service Calls via the Interactive service desk or Customer Portal in accordance with Interactive's

(j) standard procedures.

(k) Advise Interactive if any hardware or software becomes unsupported or if maintenance is terminated.

(l) Perform certification and functional testing of the vendor application patches and hot fixes for Devices.

(m) Provide Interactive access to security policy documentation related to access to the Onsite Location (where applicable) and to the Devices.

(n) Ensure an anti-virus solution is deployed and maintained on all Devices.

(o) Provide access to vendor and third-party contact details.

(p) Initially place all Priority 1 and 2 Service Calls directly via phone.

(q) Pay all third-party licensing costs required to provide Managed End User Device Services.

(r) Upon request, engage the hardware vendor to upgrade the system BIOS if applicable.

(s) Be responsible for changes occurring to their network services to enable management where those devices are not directly managed by Interactive, unless Interactive is already providing these services under a separate Statement of Work.

(t) provide Interactive with a list of current Users so they can be added as contacts to Interactive service tools.

(u) ensure sufficient spare parts for Devices are stored at each of the Remote and Onsite Locations to enable Interactive to coordinate and liaise with the relevant hardware maintenance provider where required.

(v) The Customer must acquire its own license for the use of the MDR Tool and provide Interactive with access to it to enable Interactive to leverage the MDR Tool to provide the Managed End User Device Services.

(w) Pay for any third-party tool required for Interactive to provide the Managed End User Device Services.

(x) In the case of enabling Automated Device Enrolments (ADE) on Apple Devices (MacOS, iPad OS, iOS), must sign up with Apple (vendor) for Apple Business Manager. Apple Business Manager is a complimentary service offered by Apple.

4.8 The Customer is responsible to meet all costs for:

(a) Hardware and software upgrades, licenses, subscriptions, vendor support, hardware and software maintenance, and directory management.

(b) Network connections and upgrades to network connections to support all desktops.

(c) And any other Out of Scope service expense.

5. Transition Project

5.1 Transition

(a) Interactive will follow a structured phased approach to transition the Customer to the Managed End User Device Services (the "**Transition Project**").

(b) The phases of the Transition Project are as follows for all Managed End User Device Services other than AVD and BYOD:

Transition Service	Description	Outcome
Phase 1: Transition Kick-off	Introduction meetings, expectation setting, stakeholder management, discussing roadmaps, milestones etc.	Up to 2 meetings with the Customer
Phase 2: Planning and Discovery	Auditing (current desktop/mobile environment, licensing, ticket volumes, 3rd party involvement)	(a) Up to 2 workshops (b) One "As-built" document
	Business requirements, workflow definitions, service levels, contracts, vendors, subsidiaries	
	Planning (Project scope/eligibility/timeline/deployment)	
	Reporting (Discovery, recommendation, remediation, application competency, supportability)	
Phase 3: Design, Knowledge Transfer and Documentation	Requirements gathering (Business/Users), Design assessment	(a) Customer provided: (i) Knowledge articles, (ii) Operations/Support document. (b) One Design Document
	Support system documentation gathering (system architecture/operation model/scripts)	
	Decision making process (new application onboarding process/bug fix/Change request/release management)	
	Knowledge transfer sign-off	

Phase 4: Service Establishment And Pilot	**Service Establishment (setup):** (a) MOE: Technical build and setup (b) Core App Packaging (Microsoft, Adobe) (c) Setup & Integration with MDM tool (d) Integration with ITSM tool (e) Setup TeamViewer & Verify TeamViewer access. (f) User Access Management (g) Device Security Setup (h) Mobile Device Setup **Pilot setup:** (a) Service Readiness and Testing (b) Test case implementation (c) User Feedback	**Service Establishment Outcome:** Service Documentation including Policy, Configuration, Setup instructions. **Pilot Outcome:** (a) Test Results (b) Survey Results (c) UAT Feedback
Phase 5: Operate	Service Transition Sign-off and Go-Live. Interactive will move all Services into production and advise the Customer of the Service Start Date.	Transition Sign-off & Support documents

*** Note: The phases of the Transition Project for each of AVD and BYOD is set out in the relevant Service Specification.**

(c) The timing of the phases, including whether any phases are run in parallel will be determined by Interactive.

5.2 The following are excluded from the Transition Project:

(a) Setup, enhancement, or customization of ITSM Tool.

(b) Functional testing of Applications.

(c) All other work or services not included in Service inclusions are excluded.

6. General Assumptions

6.1 The following assumptions apply in addition to any specific assumptions set out in the individual Service Specifications:

(a) Interactive will support up to one Tenant per Customer. Any additional effort will be charged at the Standard Charge Out Rate.

(b) Devices have valid hardware maintenance in place.

(c) Current anti-virus is installed by the Customer and can be centrally managed.

(d) Remote support tools are already installed and centrally managed.

(e) Operating system and Applications are configured and can be managed centrally/remotely.

(f) The Customer's asset register is accurate as at the Service Start Date, and the Customer has provided updated information to Interactive as and when required during the Individual term.

(g) If the Customer conducts any site audits that identifies any Devices or updated Device information, the Customer will provide that information to Interactive.

(h) Appropriate access will be granted to the IT environment to provide support to all Devices.

(i) Any available Application policies and existing documentation will be provided to Interactive.

(j) Incidents that require resolution by the Customer or its third-party partner or supplier, will be communicated by Interactive via email to the Customer or applicable third-party, or via an agreed process.

(k) Only Level 1 Support to be provided to SaaS application applied to non-MOE Applications

(l) Scope includes Desktop/ Laptop: Windows 10/Windows 11 and MacOS. Mobile Devices: iOS (iPhone/iPad) and Android (Samsung only).

6.2 Interactive will provide the Managed End User Device Services to the Customer either directly, via a third-party engaged by Interactive on behalf of the Customer, or both.

6.3 Interactive may deliver the Managed End User Device Services from any Interactive Facility.

7. Service Exclusions

7.1 Below items are not included in the scope of the Managed End User Device Services:

(a) Procurement, data erasure or disposal of Devices.

(b) Device refresh.

(c) Software license provisioning, recording, and tracking.

(d) Audits of any Customer sites.

(e) Support of devices not owned by the Customer or that do not utilise the MOE.

(f) Training.

(g) Change Management outside of the scope of the Managed End User Device Services, including Changes

(h) instigated or required by, or in connection with, the Customer's third-party partner or vendor.

(i) Telephone or fax systems support.

(j) Cabling infrastructure at the Customer's Onsite location

(k) Support of all other applications beyond the known Application tiers.

(l) Performance testing of Applications on new hardware.

(m) Backup of data, including data stored locally on workstations.

(n) Consumables management (Consumables means supply items such as film, toner, developer, optical exposure lamps, glassware, paper, ribbons, fuser, consumable kits, hammer springs or accessories that may be used in connection with the Customer Equipment.)

(o) Remedial (break/fix) of Devices or preventative hardware maintenance or support. Interactive can provide such services under a separate Statement of Work for hardware maintenance services.

(p) Installation of application software or third-party software patches, except as part of MOE Management or Patch Management.

(q) Interactive recommends the Customer purchase Managed Detection and Response ("MDR") services under a separate Statement of Work, with other additional options that include End Point Detection Response ("EDR") services and BYOD Security. Interactive can provide these additional services under separate Statements of Work.

(r) Network maintenance or support (including LAN / WAN / Wi-Fi). Interactive can provide such services under a separate Statement of Work. Any costs or effort for integrations or case exchange between the Interactive service management toolset and the Customer toolset or Customer third-party toolsets.

7.2 Interactive is not responsible for any failure to provide Managed End User Device Services to the extent the failure is caused, or contributed to, by any one of more of the following:

(a) the Customer not providing access to the IT Environment as required by Interactive;

(b) the Customer, its contractors, representatives' suppliers or partners, including where one or more of such persons are not co-operating or acting promptly to resolve Incidents as required (and the Customer acknowledges that, if an Incident occurs that impacts the Managed End User Device Services, it may not always be immediately apparent which of the Customer's suppliers or partners are responsible for such an Incident).

(c) any Changes or Incidents caused, or contributed to, by the Customer or third parties (except third parties engaged by Interactive).

(d) Force Majeure events.

(e) communication links; or

(f) by any Third-Party Fault.

7.3 Anything not specified as being part of the Managed End User Device Services is not included in the scope of the Managed End User Device Services. The following is a list of items that are Out of Scope, and is not intended to be an exhaustive list:

(a) Identity Management and Azure AD management;

(b) Endpoint device protection;

(c) Any travel to sites other than specified;

(d) Lodging tickets into application vendors' or the Customer's toolsets;

(e) Removal and / or secure destruction of hardware;

(f) Software licensing;

(g) Any costs or effort for integrations or case exchange between the Interactive service management toolset and the Customer toolset or Customer third-party toolsets; and

(h) Managed End User Device Services on any Public Holidays.

7.4 Except for guarantees that cannot be excluded by law, Interactive expressly disclaims all guarantees and warranties, whether express, implied or otherwise, including without limitation, guarantees of merchantability, quality and fitness for a particular purpose in respect of any Third-Party Software. Interactive does not guarantee or warrant that the Third-Party Software will be available, uninterrupted or error free, meet the Customer's requirements, or operate with the combination of hardware and software the Customer intends to use, including Managed End User Device Services.

7.5 Interactive is not required to provide "how to" articles, FAQs, service, and software updates or address the Customer's software configuration, performance issues, the Customer's desktop connectivity or service availability issues. These services may be available at an additional charge if agreed between the parties.

8. Pricing

8.1 The monthly Service Fee for Managed End User Device Services is calculated based upon the agreed number of Devices under management as set out in clause 1 of the CMS SOW. If the Customer adds any additional Devices, standard rates from the service catalogue will apply.

8.2 Monthly Service Fees for Managed End User Device Services are payable by the Customer from the Service Start Date. Interactive will issue invoices to the Customer for the Managed End User Device Services monthly in advance.

8.3 Interactive may adjust the Service Fee annually for each of the Services detailed in the CMS SOW (for the avoidance of doubt, this change applies to both initial and additional Services) by giving no less than 30 days' notice to the Customer.

8.4 The Service Fees for the Managed End User Device Services is based on the quantity of Devices specified in the CMS SOW.

8.5 Interactive may vary the monthly Service Fee when a variation to the Services is necessary due to Changes in the Customer's volumes, and this shall occur as either an addendum to the CMS SOW or in accordance with the Change Management Process.

8.6 The monthly Service Fees payable for Onsite Desktop Support are as set out in the CMS SOW.

9. Service Specification – Application Packaging Services

9.1 Interactive will provide the Application Packaging Services to enable an end-to-end in-scope service for the packaging of the Customer's end user software Applications into standardized format suitable for all enterprise software deployment and management systems ("**Application Packaging Services**"). The Application Packaging Services will only be delivered to in-scope Devices and Applications.

9.2 The Application Packaging Services consist of the following:

(a) Requirement gathering for Application Packaging.

(b) Creating packages of software following the Customer standards for all eligible software.

(c) Releasing Customer nominated system software and Applications into production.

(d) Retire Customer nominated Applications and system software.

9.3 Packages must meet the Customer defined Application Packaging standards and policies provided to Interactive by the Customer.

9.4 During the Transition Project the key solution inputs that the parties must agree include:

(a) The number of Application Packages that Interactive is required to create per month.

(b) The complexity split of applications – i.e., Simple vs Medium vs Complex (as defined in clause 9.8).

(c) The number of MOEs to be supported.

9.5 A new Application Package will be created for all in scope Applications in the following circumstances:

(a) The Customer has notified Interactive of a security vulnerability related to an Application and requests an update for the Application be deployed to User Devices.

(b) Interactive has advised the Customer of a vulnerability or compatibility issue and the Customer requests an update for the Application be deployed to User Devices.

9.6 If the Customer requests that additional Applications be added to the scope Interactive will deploy the additional User Devices at an additional charge.

9.7 The following assumptions apply to the Application Packaging Services:

(a) All the existing Applications have been pretested to be compatible on Windows 10/Windows 11 and MacOS.

(b) A maximum of one new Application request (Simple Applications only) is to be considered for packaging every month. Any additional request will require additional effort and will be managed as on-demand/POA.

(c) The Customer will perform all Application compatibility testing for any new Application Package request.

(d) Testing will be carried out by deploying to one master image.

(e) All Application Packages are in ENGLISH language only.

9.8 Application Package Complexity analysis and categorization (Simple, Medium, or Complex):

(a) Interactive categorizes Application Packages as simple, medium and complex based on the level of customization required to package them as well as the complexity of Applications being packaged. The following definitions apply:

(i) Simple means: Applications that do not require any modification and that can be uploaded to the MDM tool without Packaging. Typical file formats for Simple Applications are .MSI. Examples of Simple Applications are Microsoft Office, Adobe Acrobet.MSI downloaded from the vendor website.

(ii) Medium: Any Applications format that are not listed as simple which Interactive is required to Package. For example, Single EXE (no customization).

(iii) Complex: Applications that require Interactive to bundle multiple installation files and customise e.g., Simple EXE with customization, multiple MSIs, MST, batch files.

9.9 The following Exclusions apply to the Application Packaging Services:

(a) Any Application Packaging outside of the following is not available: Application Packaging Services are only available on MOE Windows 10/Windows 11 devices and MacOS only.

(b) Packaging of only Simple Applications (.MSI or .exe) is included under the standard scope of the Application Packaging Services. Packaging of Medium and Complex Applications will be charged as price on application.

9.10 Customer Responsibilities

(a) The Customer must:

(i) Provide Interactive with all necessary Vendor Application sources.

(ii) Utilise the Intune Agent in their environment.

(iii) Maintain the Workstation Agent Health data within its Azure Microsoft subscription.

(iv) Provide Interactive administrative access to the Intune environment.

(v) Provide Interactive with Application Packaging requirements and instructions.

(vi) Provide the staging and testing environment.

(vii) Perform all functional testing of new Application Packages.

(viii) Provide Interactive with the User Acceptance Test ("**UAT**") Plan.

(ix) Perform UAT testing and Application Packaging sign off to enable Interactive to deploy into production.

9.11 The table below sets out the high-level responsibilities between the Customer and Interactive for Application Packaging:

Task	Interactive	Customer
Demand Phase		
Package Request: accept the submitted request review for the required information: - SourceMedia - Installation Instructions - Application Owner - License Information - Application lifecycle management"	R	A
Demand Lead - Follow Request from start to finish	AR	C
Document Request Information	AR	C
Packaging Phase		
Verification of Source media - Source Validation	AR	I
Package Prioritization - Business Critical (P1)	C	AR
Package Prioritization	AR	C
Coordinate information gathering sessions with Requestor/Vendor	AR	C
Package Creation in line with Business Requirements	AR	I
Package Troubleshooting - during the creation and/or testing of a package: - Answer questions from the requestor - Troubleshoot and resolve any issues uncovered during build and testing	AR	C
Package retirement	C	AR
Maintain a development/test environment	CI	AR
Provide development, testing tools and licenses	C	AR
Software Package Creation, testing and Distribution process and tool definition	C	AR
Package Review	R	A
Testing Phase		
Perform testing activities in required timeframe	AR	C
Document testing and signoff	AR	C
Testing review	R	A
User Acceptance Testing		
Perform install test and verify requests were met - Facilitate testing with the identified tester to perform functional testing	C	AR
Initiate UAT - Facilitate testing with the identified tester to perform functional testing	C	AR

Certify and Publish Package to Production: - Receive UAT approval from requestor/tester/application owner - Promote the package into the production environment	AR	C
Testing Review	R	A

10. Service Specification – Software Distribution Services

10.1 Interactive will provide Software Distribution Services to the Customer which consists of the following ("**Software Distribution Services**")

(a) Automated remote distribution of software on the Devices leveraging the Customer's existing network infrastructure.

(b) Interactive may (at its discretion, and as necessary to ensure business continuity) install software on the Devices.

(c) Deployment process customization and co-ordination.

(d) Package conflict detection and resolution, applicable for complex packages only.

(e) Deployment to distribution groups (phase wise devices).

(f) Liaison with network and/or security teams and /or vendor to resolve deployment issues, if any.

10.2 Interactive and the Customer will work together to nominate the Devices for pilot deployment. Interactive will perform the pilot deployment on the nominated Devices.

10.3 During the Transition Project the key solution inputs that the parties must agree include:

(a) The number of Applications to be deployed per month.

(b) The number of MOE's to be supported.

10.4 Customer Responsibilities:

(a) The Customer must:

(i) Provide Interactive with the application distribution groups.

(ii) Perform UAT testing.

(b) Ensure that Network connectivity is available and appropriate firewalls ports are opened for the software distribution. Windows devices and Mac devices are enrolled in the MDM Tool, and devices are online to receive the application package distribution.

10.5 The table below sets out the high-level responsibilities between the Customer and Interactive for the Software Distribution Services:

Software Distribution Tasks	Interactive	Customer
Assign a deployment point of contact	AR	C
Plan pilot	A	RCI
Create pilot deployment	AR	CI
Ensure pilot communication is sent	A	RCI
Create deployment Change request	C	AR
Plan deployment	R	A
Create and maintain deployment report	AR	C
Initiate draft Change in ServiceNow	I	AR
Approve Change	I	AR
Ensure Change is approved before deployment start	R	A
Inform of start deployment	R	A
Add deployment waves/machine list to collection	R	A
Monitor deployment	R	A
Report deployment status	R	A

11. Service Specification – Remote Desktop Support

11.1 Interactive will provide remote desktop support to the Users, which consists of the following for each Remote Location ("**Remote Desktop Support**"):

(a) Respond to and/or raise tickets and attempt to resolve Incidents (L3 only) or assign and escalate the ticket where required.

(b) Installation, moves, adds, Changes (IMAC) for the Devices, subject to clause 1.8.

(c) IMAC Requests: Install, Move, Add, Configure Services:
Interactive will perform IMAC Request as part of standard desktop service offering which consist of the following:

(i) Coordinate the installation of PCs, peripherals and LAN-based equipment.

(ii) Setup security, file access and other administrative procedures associated with moves.

(iii) Install non-network software for Users in local sites.

(iv) Ensure that basic connectivity issues are addressed.

(v) Consult with Users to identify and clarify their needs specific to Applications/new requirements etc.

(vi) Consult with third-party vendors for recommendations and options to satisfy Users' needs.

(vii) Identify incompatibilities among the Users' Applications needs and the established infrastructure and provide a solution to resolve.

(viii) Prepare and submit required documents to initiate orders for equipment, software and third-party services.

(ix) Perform end-user notifications (for location specific outages/ updates), if required in addition to central notification from the service desk.

(d) Configuration and management of print queues for Users.

(e) Configuration and support for printer policy and printer mapping.

(f) Configuration and management of universal print drivers.

(g) Active Directory User Account administration (creation, deletion, Changes, password resets).

(h) User desktop profile support (creation, Changes, availability).

(i) Microsoft Outlook profile support (excludes PST file issues).

(j) Network user logon services support (Network logon, group policy settings, logon scripts).

(k) Network folder access support, excluding 3rd party cloud hosted platforms.

(l) Mailbox administration (creation, deletion), excluding mail archiving, hosted Exchange and Office 365 platforms.

(m) Malware and virus removal for devices/OS under management. This assumes appropriate security measures are in place.

11.2 Interactive will provide the Remote Desktop Support during the Business Hours.

(a) The Customer must nominate a "Site Champion" for each Remote Location, who will:

(i) be the key liaison point with Interactive.

(ii) manage and take responsibility for any spare equipment; and

(iii) provide Interactive with all relevant Device Information necessary to enable Interactive to maintain the Asset Register for the Remote Location, which the Customer must provide to Interactive at least monthly or as otherwise agreed between the parties.

11.3 The following assumptions apply to the Remote Desktop Support:

(a) Operating system and Applications are configured and can be managed centrally/remotely.

11.4 The following are excluded from the Remote Desktop Support:

(a) Any device that is not part of agreed in scope.

(b) Restoration of available backed up network files and mailbox items.

11.5 The table below sets out the high-level responsibilities between the Customer and Interactive for Remote Desktop Support:

Task	Interactive	Customer
Attend to the Level 3 tickets which are escalated from Level 2 teams, including the Service Desk and/or Onsite Support teams	RA	CI
Diagnose, troubleshoot, resolve and escalate in-scope supported software, hardware and peripheral Incident calls escalated from Service Desk team in accordance with Service Levels established	RA	CI
Adjust configuration options as required to resolve defects identified during testing and while performing corrective action on a device	RA	CI
Investigate incidents that are in scope and identify root causes to be able to provide solutions	RA	CI

12. Service Specification – Patch Management Services

12.1 Interactive will remotely apply security and feature Updates to Devices during maintenance windows agreed with the Customer as follows ("**Patch Management Services**"):

(a) Microsoft operating system patching – Critical security patching only once every month.

(b) Microsoft Office Applications will be patched in alignment with vendor released Updates every month.

(c) Vendor escalation for software faults and bugs.

(d) Release of MacOS vendor released Updates in alignment with the vendor specifications.

(e) Patching to any third-party software is restricted to a maximum of one software Application per month.

12.2 Interactive will follow the below Patch Management process:

(a) Define the baseline patch levels.

(b) Search for new Updates/patches on monthly basis.

(c) Deploy patches at Interactive's discretion.

(d) Perform patch testing.

(e) Deployment of patches to the distribution groups that the Customer has predefined.

(f) Tracking success rate of patching.

(g) Liaison with vendor to resolve complex issues.

12.3 Applicable Service Level Target

(a) Interactive will aim to patch 90% of online Devices with Updates within 30 days after the Update is released.

12.4 The following assumptions apply to the Patch Management Services:

(a) All Devices are enabled to receive the Updates via automated processes.

(b) The Customer will agree to a scheduled maintenance window for Updates to be applied.

(c) Within the Customer environment there is an MDM Tool already installed, configured and with Devices enrolled to it.

(d) The Customer will ensure that Devices are made available to Interactive during the patching cycle.

12.5 The following are excluded from the Patch Management Services:

(a) Any applications or operating systems not on the MOE.

(b) Upgrades to the next major release of an operating system or Application.

(c) Operating systems and Applications that are not in scope.

12.6 Interactive is not liable for any risk associated with a patch or the vulnerabilities the patch intends to fix if the Customer and Interactive have not agreed to a patch window within 30 days of Interactive notifying the Customer about the patch.

12.7 Interactive only applies Updates made available by operating system or application vendors and Interactive cannot guarantee the Updates will address vulnerabilities or be free from defects.

12.8 The Customer shall provide personnel for testing during the patch window as required to test the environment (which may include applications) after the patch is deployed.

12.9 The table below sets out the responsibilities between the Customer and Interactive for the Patch Management Services:

Task	Interactive	Customer
Definition		
Definition of patch waves per month	CI	RA
Configuration of tooling to match the patching definition	RA	CI
Patch Management		
Patch scheduling	RA	IC
Patch installation	RA	IC
Patch issue reporting	IC	RA
Post-patch testing	IC	RA
Patch compliance reporting	RA	CI
Monthly deployment of patches and version updates for supported applications	RA	CI
Monthly compliance reporting on patch levels and devices licensed.	RA	CI
Troubleshooting of compatibility between new versions of Applications	CI	RA
Troubleshooting of vendor software bugs introduced by Updates excluded	CI	RA

13. Service Specification – Device Security Management

13.1 Interactive will provide the following Device Security Management Services (as determined by Interactive) which consists of the following ("**Device Security Management**"):

(a) Configuration of the Customer Devices with the following security configurations:

(i) User passwords.

(ii) Application Protection.

(iii) Compliance policies.

13.2 Exclusions:

The following are excluded from the Device Management Services:

(a) Enhanced Device security such as Managed Detection and Response. MDR is available as an additional service at an additional charge from Interactive under a separate Statement of Work.

14. Service Specification – Managed Operating Environment ("MOE")

14.1 Interactive will provide the following Managed Operating Environment Services ("**MOE**") which consists of:

(a) Assessment and requirement gathering of the Device estate.

(b) Develop the MOE.

(c) Manage and maintain an MOE, with Windows 10/Windows 11, including core Applications and compliance policies, as defined during the Transition Project (or as may be otherwise agreed with the Customer).

(d) Provision Devices and in-scope apps on Devices.

(e) Technical support for service restoration.

(f) Troubleshooting and resolution of the Customer's operating system performance issues.

(g) Desktop operating system re-installation/re-builds on existing machines.

(h) Assign profiles.

(i) Monitor profiles.

(j) Issue tracking and resolution.

(k) Vendor escalation for standard core supported applications.

14.2 The following assumptions apply to MOE Management:

(a) Hardware in use (including Devices) and core applications will be supported by the MOE, including any updates to it.

(b) Operating system and applications on the MOE have current vendor support agreements in place.

(c) The Customer will agree to a scheduled maintenance window for Updates to be applied.

14.3 The following Customer obligations apply:

(a) The Customer must procure and dispose of the Devices.

14.4 The following exclusions apply to the MOE and MOE Management:

(a) Physical relocation of user machines and peripherals for desk moves.

(b) Troubleshooting of compatibility between new versions of the operating system.

(c) Troubleshooting of vendor software bugs introduced by Microsoft/Apple for Desktops/Laptops.

(d) Updates to non-standard Package Applications.

(e) Packaging and/or installation of non-standard Applications.

(f) Windows XP, Windows 7 – No support.

(g) Application functionality testing and validation.

(h) Application development or enhancements.

(i) Any Applications or operating systems not on the MOE.

14.5 The table below sets out the responsibilities between the Customer and Interactive for the Managed Operating Environment Services:

Activities	Interactive	Customer
Define the MOE requirements	CI	RA
Develop and document detailed technical specifications that define and support the build, test and deployment plans for the master image	RA	CI
Development and testing of master image	RA	CI
Create the build document including the MOE details and deployment procedures that meet the Customer requirements as defined during the Transition Project	RA	CI
Update the document which includes the MOE Changes and deployment procedures that meet requirements.	RA	CI
Update and maintain master image as per Customer requirements defined during the Transition Project	RA	CI
Review and approve security policies and patches	RA	CI
Review and approve all patches and Windows 10/Windows 11 feature Updates	RA	CI
Deploy all the patches and Windows 10/Windows 11 feature Updates	RA	CI
Coordinate the implementation of security policies on all Devices	RA	CI

Provide agreed releases per year for each master image	RA	CI
Collate patch information i.e., list of included / excluded Microsoft patches	RA	CI
Integrate new Devices brand/model into the current master image	CI	RA
Provide nominated Users for user acceptance testing	CI	RA
Ensure that the performances of the new master images are better or equivalent to the previous ones.	RA	CI
Review and approve master image testing results.	RA	CI
Approve master images for deployment.	CI	RA
Provide tooling necessary to deploy and maintain the image to support the Managed End User Device Services.	CI	RA
Define, strategize and decide on the deployment strategy for the Windows 10/Windows 11 features, patches and Windows servicing models	RA	CI
Solve technical issues related to operating system and standard software component	RA	I
Troubleshoot system performance, group policy and bit locker related client-side issues	RA	I

15. Service Specification – Device Lifecycle Management

15.1 For the purposes of this this Service Specification Devices only includes Managed Desktops and laptops that have been enrolled into the MDM Tool. It does not include mobile phones, tablets or thin clients.

15.2 Interactive will provide Device Lifecycle Management for the Devices, which consists of the following ("**Device Lifecycle Management Services"**):

(a) Hardware vendor co-ordination

If required, for up to 5% of the overall Device estate, Interactive will assist the Customer in discussions with the Device vendor for coordination of Device procurement. The Customer, not Interactive, must procure Devices and hardware parts directly from the vendor. For example, out of every 100 Devices, Interactive will provide vendor co-ordination support for up to 5 Devices every month. Any additional effort will be charged at the Standard Charge Out Rate.

(b) Asset Inventory Management.

15.3 Interactive will provide Asset Inventory Management Services ("**Asset Inventory Management**") which consists of the following:

(a) Maintaining an inventory of all in-scope User Devices and track any Changes to these Devices within the ITSM Tool, including the Devices' make and model, location, ownership, status and Asset tag (where available).

(b) Interactive will create and maintain the Asset Register for the Devices. Interactive will maintain the accuracy and completeness of the Asset register for the Devices by updating it regularly, when Devices Change state, or when the assignment of a Device Changes as part of User onboarding and offboarding.

(c) The Asset Register will contain the following information deemed necessary to identify the Device assigned to each of the Users. Interactive will ensure that each in-scope Device is properly catalogued within the Asset Register, including the following information:

(i) Configuration Item / Asset ID.

(ii) Device Make and Model.

(iii) Asset Owner / Assigned to Person.

(iv) Assignment Date.

(v) State / Status / Sub-State.

(vi) Site Location.

(vii) Stockroom Location.

(viii) Warranty Expiration Date.

(ix) Install Date.

(d) Interactive will conduct periodic audits (in conjunction with the Customer) of all in-scope User Devices to ensure that the inventory is accurate and up to date.

(e) Interactive will provide regular reports on Device inventory and tracking in accordance with the process with the Customer which shall include information on Device ownership, location, status, any Changes that have been made to the Devices and the stock room inventory volumes.

(f) The following assumptions apply to Asset Inventory Management Services:

(i) The Customer's asset register is accurate as at the Service Start Date and the Customer has provided updated information as and when required during the Individual term.

(ii) If the Customer conducts any site audits that identify any Changes to Devices or Device information the Customer will provide that information to Interactive by engaging the Service Desk.

(iii) The Customer will provide Interactive with any information pertaining to its asset register or existing spares pool for each Remote Location.

(iv) The Customer will advise Interactive of any lost, stolen, or defective Devices that are in scope of support by engaging the Service Desk.

(v) The Customer will manage Asset tagging requirements with their hardware vendor and provide Interactive any relevant information as required.

(vi) The Customer's nominated site contacts for each geographic region/location must:

A. Be the key liaison point with Interactive for items pertaining to Asset Inventory Management Services for that region/location.

B. Manage and take responsibility for any spare equipment in the Remote Location spares pool.

C. Ensure that the spares pool is kept fulfilled as required in accordance with the process agreed during the Transition Project, based on guidance from Interactive; and

D. advise Interactive via the Service Desk of any issues pertaining to the spares pool or supported Devices.

(g) Asset Disposal Services are not included in the scope of the Managed End User Device Services. If the Customer requires Asset Disposal Services, it may engage directly with Interactive's subsidiary company Erase IT under a separate agreement.

(h) The Customer will engage Interactive via the Customer Portal, phone or email with their requirements, should any scoping be required for Device refresh activities or project work. Interactive will respond with a quote for the additional work and if the Customer accepts the quote the parties will enter into a separate statement of Work for the additional work.

(i) The following exclusions will apply to the Asset Inventory Management Services:

(i) Integration with the Customer's CMDB or asset register(s).

(ii) Tracking of any financial data or depreciation information.

(iii) Tracking of any information pertaining to agreements/contracts between the Customer and their partners or third parties.

(iv) Device lifecycle management relating to procurement, logistics, third-party contracts and Asset refresh programs.

(v) Device lifecycle management relating to physical Asset deployment, secure wipe and disposal.

(vi) Physical Asset deployment to any Remote Locations.

(vii) Software license recording and tracking of any software that is not part of the MOE.

(viii) Physical audits of any Customer site.

(ix) Mobile devices (including tablets) not included under management of the in-scope support services.

(x) Consumables or peripherals.

(xi) License management.

(xii) Insurance relating to the shipping, transfer, or postage of Devices during physical deployment or other times.

(xiii) Devices that are Dead on Arrival.

(xiv) Devices that are not enrolled into and managed via Intune.

(xv) Tracking and management of items such as cables, adaptors, screens, monitors, docking stations, keyboards, power boards, mice and anything not stated as a supported device.

(xvi) Interactive will perform the Asset Inventory Management Services for a maximum of 2 hours per month. Any additional effort will be charged at the Standard Charge Out Rate

(j) Operating system upgrades:

(i) Interactive will perform up to two operating system upgrades in a year on supported in-scope Devices in alignment with the vendor and the Customer.

(k) Hardware Break/Fix Co-ordination only:

If required, for up to 5% of the overall Device estate, Interactive will provide the following services:

(i) Assist the Customer to resolve hardware related issues with the vendor (escalated by the Interactive Service Desk).

(ii) Interactive will act as the interface between the Customer and the hardware vendors for planning and problem resolution.

(iii) Interactive will perform the Hardware / Break fix Co-ordination for a maximum of 0.5 hours per Device. Any additional effort will be charged at the Standard Charge Out Rate.

(l) Escalated Support to the Level 3 Team for issues with Customer Devices.

(i) Where an issue cannot be resolved by the Service Desk it will be escalated to the Level 3 Team.

(ii) Interactive will perform the escalated support for up for a maximum of 5% of the total ticket volumes per month per Device. Any additional effort will be charged at the Standard Charge Out Rate. For example, out of a total of 100 EUS incident tickets per month, up to 5 EUS incident tickets (Level 3) could be escalated to the Managed End User Device Services team for support and resolution.

15.4 The following exclusions apply to the Device Lifecycle Management:

(a) Virtual Apps and Virtual Desktops.

(b) Application functionality testing and validation.

(c) Application development or enhancements.

(d) Break/Fix of Devices (other than the co-ordination efforts described in clause 15.2.

(e) Warranty management of Devices.

(f) License management of operating system.

(g) Integration with the Customer's configuration management database.

16. Service Specification - Reporting

16.1 Interactive will provide Reporting for Managed Desktop and laptops:

(a) Service Level Report:

(i) Provide a monthly Service level Agreement report. This report will include the Incident Service Levels, the Patch Service Levels and the number of Service Requests. Interactive's effort in producing the report will not exceed 1 hour per report per month. If the Customer requests any additional reporting Interactive will charge an additional fee at the Standard Charge Out Rates.

(b) Device Reporting (Technical)

(i) Provide a monthly technical report on the number Devices enrolled in the MDM Tool highlighting the enrolment status of Devices and compliance of Devices. Interactive's effort in producing the report will not exceed 1 hour per report per month. If the Customer requests any additional reporting Interactive will charge an additional fee at the Standard Charge Out Rates.

17. Service Specification – Onsite Desktop Support

If the CMS SOW states that the Customer has purchased Onsite Desktop Support, the following applies:

17.1 Interactive will provide the number of resources set out in the CMS SOW to provide the following services at the Onsite Location as specified in the CMS SOW ("**Onsite Desktop Support**"):

(a) Respond to, and, where required, raise tickets and attempt to resolve incidents, or assign and escalate the ticket to the appropriate resolver team.

(b) Execute Service Requests, which will be prioritised based on the capacity of the onsite resource or assigned to other resolver teams as required.

(c) Management of print queues on the Devices. Only Universal print divers are in scope.

(d) Management of User component of Active Directory group membership.

17.2 The Onsite Desktop Support will be provided during Business Hours.

17.3 Notwithstanding the Individual Term, Interactive will provide the Onsite Desktop Support, commencing from the Service Start Date for the Individual Term for the number of Days or Hours specified in the CMS SOW (or such other date as may be agreed by the parties, or failing agreement a date specified by Interactive).

17.4 The following assumptions apply to the Onsite Desktop Support:

(a) TeamViewer is in use for remote support.

(b) For the duration the Onsite Desktop Support is provided, there is no cap on Service Requests that can be performed by the onsite resource. Onsite Desktop Support provided is limited by the capacity of the onsite resource.

(c) For the duration the Onsite Desktop Support is provided, IMACs (Installation, moves, add, Changes) will be prioritised based on the capacity of the onsite resource.

17.5 Customer Responsibilities

The Customer must:

(a) log support tickets via the Customer Portal;

(b) provide OHS training and site induction for the onsite resource;

(c) provide the onsite resource with a dedicated workspace at the Onsite Location, with laptop, office space and desk;

(d) nominate a "Site Champion" for the Onsite Location, who will:

(i) be the key liaison point with Interactive.

(ii) manage and take responsibility for any spare equipment; and

(iii) provide Interactive with all relevant Device Information necessary to enable Interactive to maintain the Asset for the Onsite Location, which the Customer must provide to Interactive at least monthly or as otherwise agreed between the parties.

17.6 The following are excluded from the Onsite Desktop Support:

(a) Travel to any locations other than the Onsite Location.

18. Service Specification – Managed Mobility Services

If the CMS SOW states that the Customer has purchased Managed Mobility Services, the following applies:

18.1 Reporting: Interactive will provide Reporting for Mobile Devices.

(a) Device Reporting (Technical)

(i) Provide a monthly technical report on the number and type of Mobile Devices enrolled in the MDM Tool highlighting the enrolment status of Mobile Devices and compliance status of the Mobile Devices. Interactive's effort in producing the report will not exceed 1 hour per report per month. If the Customer requests any additional reporting Interactive will charge an additional fee at the Standard Charge Out Rates.

18.2 Mobile Device Management:

(a) Interactive will provide the following Device Management services for the in-scope Mobile Devices.

(i) Device enrolment and configuration into MDM Tool.

(ii) User profile deployment.

(iii) Assignment into the MDM Tool.

18.3 Mobile Application Management:

(a) Interactive will provide the following Mobile Application Management services for Mobile Devices:

(i) Application Support basic troubleshooting for Microsoft native apps.

(ii) Managing upgrades for Microsoft O365 apps viz, Email client and MS Teams.

18.4 Asset Information for Mobile Devices:

(a) Interactive will upload the Mobile Device information into MDM Tool. This Information will include the Device model, Serial number, Username and operating system information. During the Transition Project, the Customer must provide a complete and current list of Users and the relevant Mobile Devices assigned to each User ("Initial List")

(b) The Initial List will form the basis of the Mobile Device information and will allow the Service Desk to identify the Mobile Devices and the relevant User. Once the Initial List is finalised and verified by the Customer, it will be hosted within the Customer Portal for the Customer to access and update.

(c) Interactive will provide a monthly report detailing the Mobile Device Information.

18.5 Mobile Security Management:

(a) Interactive will provide the following Security for Mobile Devices:

(i) Managing Corporate access for users on Mobile Devices.

(ii) Interactive will perform the Mobile Security Management Services for a maximum of 1 hour per month. Any additional effort will be charged at the Standard Charge Out Rate.

18.6 Hardware Break/Fix Co-ordination only:

(a) If required, for up to 5% of the overall device estate, Interactive will provide the following services:

(i) Resolve hardware or software related issues on a best effort basis.

(ii) Interface with hardware and software vendors for planning and incident resolution.

(b) The Customer must provide all relevant vendor details to Interactive to support hardware break/fix co-ordination.

(c) The Customer is responsible for any procurement of any hardware or software or transport of equipment.

18.7 Interactive will perform the Hardware Break/ fix Co-ordination for a maximum of 0.25 hours per Mobile Device. Any additional effort will be charged at the Standard Charge Out Rate.

18.8 User Support:

(a) Interactive will triage and attempt resolution for issues pertaining to the Customer Mobile Devices. Should it be identified that the issue falls outside the scope of this Service Description (e.g., hardware failure), the issue will be referred back to the Customer for resolution.

(b) IMAC

(i) Interactive will perform a maximum of 2 (IMAC) Service Requests per month for Mobile Devices which includes the following:

A. Setup security, user access and other administrative procedures associated with moves.

B. Consult with Users to identify and clarify their needs specific to applications/new requirements etc.

C. Consult with third-party vendors for recommendations and options to satisfy Users needs.

D. Assist the Customer Users request for a new Mobile Device.

(ii) Any additional effort requested will be charged at the Standard Charge Out Rate.

(c) Standard OS upgrades (up to 2 OS upgrades per year) in alignment with the vendor and the Customer.

18.9 The following Assumptions apply:

(a) Application issues on Mobile Devices will be redirected to the Customer.

(b) Synchronizations include email and calendar only.

(c) The Customer is responsible for any costs associated with Mobile Devices and usage plans.
e.g., The Customer will interface with the identified Telephone and Expense Management (TEM) provider for Mobile Devices.

(d) Relevant processes will be agreed between the Customer and Interactive to support these assumptions.

18.10 The table below sets out the responsibilities between the Customer and Interactive for the Managed Mobility Services:

Activities	Interactive	Customer
MDM, MAM Platform Hosting	I	AR
Vendor Co-ordination for Recycle and Repair	R	ACI
Hardware Replacement	I	RA
E-mail Setup/ Intune enrolment	RA	I
Email access & troubleshooting	RA	I
Remote wipe of device	RA	I
Mobile Device Replacement & Onboarding	I	RA
Mobile Device Disposal	I	RA
Mobile Device account Lockout/Password reset	RA	I
Mobility Tech Support: Data Sync, Wi-Fi, OS Updates	CI	RA
User group creation and maintenance	RA	I

Interface with TEM provider for catch and dispatch of tickets	I	RA
Mobile Device Testing and Troubleshooting	CI	RA
End User Support	RA	CI
Registration for Apple Business Manager or other vendor management tools	I	RA

19. Service Specification – Managed End User Device Services for Bring Your Own Device ("BYOD")

19.1 If the CMS SOW states that the Customer has purchased the Managed End User Device Services for BYOD, the following services will be provided for the in-scope Users:

(a) Service Reporting.

(b) Mobile Application Management.

(c) IT Support and Management.

(d) Mobile Security Management.

(e) Scope Inclusions:

(i) Devices: Mobile, Tablet, Laptop.

(ii) Operating System (OS): iOS, Android, MacOS and Windows platforms.

(iii) Compatible OS versions as supported by the vendor/OEM.

19.2 Reporting: Interactive will provide Reporting for BYOD Service.

(a) **Service Reporting**:

(i) Interactive will provide a monthly report on:

A. the status of access termination, application wipes, in the case of the Customer User's ~~BYOD~~ personal device being stolen or lost, or if the User has left the Customer's organisation.

B. The list of all Applications on the BYOD (assuming the device is enrolled into MDM tool)

(ii) Interactive's effort in producing the report will not exceed 1 hour per report per month.

(iii) If the Customer requests any additional reporting Interactive will charge an additional fee at the Standard Charge Out Rates.

19.3 **Mobile Application Management:**

(a) Interactive will provide the following Mobile Application Management services for BYOD:

(i) Managing access to managed Applications.

(ii) Restricting interaction between managed Applications and unmanaged applications.

(iii) Revoking licenses for managed Applications when Users no longer require them.

(iv) Application containerization to segregate the work and personal profiles of the Users.

19.4 **IT Support and Management:**

(a) Interactive will provide the following IT Support services for the in-scope BYOD.

(i) Ongoing support, (i.e., availability and accessibility), for managed Applications.

(b) **User Support:**

(i) Interactive will triage and attempt to resolve issues pertaining to the Customer BYOD Users. Should it be identified that the issue falls outside the scope of this Service Description (e.g., hardware failure, device related issues, installed Applications etc.), the issue will be referred to the Customer for resolution.

(ii) Service Request for new Users:

A. Interactive will perform a maximum of 2 Service Requests per month for BYOD Service which includes the following:

(i) Setup security, User access and other administrative procedures associated with new Users.

(ii) Consult with Users to identify and clarify their needs specific to Applications or requests for new requirements.

B. Any additional effort requested will be charged at the Standard Charge Out Rate.

19.5 **Mobile Security Management:**

(a) Interactive will provide the following Security for BYOD Service:

(i) Office Web Applications only for PC and Mac.

(ii) Disable printing of Customer data for managed Applications only.

(iii) Restrict copying and pasting of Customer data between managed Applications and unmanaged applications.

(iv) Provision BYOD with profiles that manage and protect work Applications and data within the managed Applications in the same manner as corporate Devices.

(v) Restrict access to M365 data based upon geo-locations as defined by the Customer.

(vi) Enforce Application protection policies.

(vii) Audit and revoke access to business Applications and emails on BYOD and encourage enrolment for secure access.

(viii) Stringent password settings for managed Applications.

19.6 **The following Assumptions apply:**

(a) All Application compatibility and functional issues on Mobile Devices will be redirected to the Customer.

(b) Security management will be performed using the following MDM controls:

(i) Intune Application Protection Policies.

(ii) Azure AD Conditional Access.

(iii) Interactive recommends additional Cyber products such as MDR (Managed Detection and Response), EDR (End Point Detection and Response) to be purchased by the Customer under a separate Statement of Work. This requires device enrolment either into MDM or Microsoft Defender for Endpoint.

(c) Relevant processes will be agreed between the Customer and Interactive to support these Assumptions.

(d) If the Customer wants to enroll their User's personal Devices into MDM, then the associated tasks need to be called out in the SOW.

19.7 **Customer Responsibilities:**

(a) The Customer is responsible for any costs associated with devices and usage plans related to the BYOD service.

(b) The Customer will interface with the identified Telephone and Expense Management ("**TEM**") provider for personal Devices.

(c) All requests for enrolling in the BYOD Service must be made through the online ITSM portal and associated processes. The Customer must ensure that the Users comply with the policies and procedures mentioned below:

(i) The operating system on the BYOD is up to date and in the form intended by the manufacturer i.e. not Jailbroken or Rooted.

(ii) Malware is not installed on the BYOD.

(iii) Personal information on the BYOD has been copied to a secure backup location if the authorised User seeks to retain the information.

(iv) mobile security (anti-virus) software is installed and configured with daily updates

(d) The Customer is responsible for the license management required for BYOD management.

(e) The Customer will be responsible for specifying the policies and procedures defining the usage of BYOD for the Users, scope including but not limited to:

(i) Device Compatibility: The Customer must specify the types of BYOD (smartphones, tablets, laptops) and operating systems (iOS, Android, Windows) that are allowed to be used for work purposes.

(ii) Access control: The Customer must define which company resources (email, specific Applications, data) the Users BYOD can access and any restrictions on accessing sensitive information.

(iii) Network usage: The Customer must specify whether the BYOD should only connect to secure networks (i.e. no public Wi-Fi) to minimise the risk of data breaches.

(iv) Regular Updates: The Customer must ensure that the BYOD are regularly updated with the latest supported OS patches to protect against vulnerabilities.

(v) Application Usage: The Customer must specify which Applications should be used for work-related tasks and whether the Users are allowed to download additional Applications for work purposes. This includes any supporting applications such as Microsoft Authenticator for iOS and Company portal app for Android devices.

(vi) Remote Wipe: Clarify the Customer's ability to remotely wipe corporate data from a BYOD in case it gets lost, stolen or when the employee leaves the company.

(vii) User Training: The Customer must train their Users on security best practices.

(viii) Compliance: The Customer must ensure that their Users adhere to industry regulations (e.g., GDPR).

(ix) Acceptable Use: The Customer must define acceptable and unacceptable uses of BYOD during work hours and in relation to company resources.

(x) Liability: The Customer must clarify the responsibilities for their Users in case of data breaches, security incidents, or other problems related to BYOD usage.

(xi) Reporting Security Incidents: The Customer must provide guidelines on how the Users should report lost BYOD, security breaches, or suspected compromises promptly.

(xii) Policy Updates: The Customer must specify how updates to the BYOD policy will be communicated to the Users and how they are expected to stay informed.

(xiii) Privacy: The Customer must clearly communicate the extent to which they can monitor or access personal data on User BYOD for work-related purposes.

(xiv) Personal Data: Interactive is not responsible for any loss of Personal Data on the BYOD due to configurations and changes applied on them.

(xv) For the purposes of clauses 19.7 (c)(e) (xiii) and (xiv)Personal Data means any data that is not the Customer's data or is not generated by or for the Customer or required by the Customer for the sole purpose of running its business activities.

19.8 The table below sets out the responsibilities between the Customer and Interactive for the BYOD Services:

Activities	Interactive	Customer
MAM Platform Hosting	I	AR
Vendor Co-ordination for Recycle and Repair	I	RA
Hardware Replacement	I	RA
E-mail Setup/ Intune enrolment	RA	I
Email access & troubleshooting	RA	I
Application Wipes	RA	I

Mobile Device Replacement & Onboarding	I	RA
Mobile Device Procurement and Disposal	I	RA
Mobile Device account Lockout/Password reset	RA	I
Mobility Tech Support: Data Sync, Wi-Fi, OS Updates	CI	RA
User group creation and maintenance	RA	I
Interface with TEM provider for catch and dispatch of tickets	I	RA
Mobile Device Testing and Troubleshooting	CI	RA
Registration for Apple Business Manager or other vendor management tools	I	RA
Expense Reimbursement	I	RA
Obtaining Legal Approvals for BYOD Usage	CI	RA
Security approvals for accessing BYOD	RCI	A
Secure Access to Corporate Network	CI	RA
Employee Education and Change Management	CI	RA
Legacy and Privacy Aspects	CI	RA
BYOD Funding arrangements	CI	RA
Decision to enroll BYOD into MDM tool supported by Interactive	CI	RA
Assist the Customer in creation of BYOD Policy for the Customer organisation	RCI	A

R=Responsible, A=Accountable, Consulted, I=Informed

19.9 Project Transition: clause 5 does not apply to the Managed End User Device Services for BYOD, instead the following phases of the Transition Project apply:

Transition Service	Description	Outcome
Phase 1: Transition Kick-off	Introduction meetings, expectation setting, stakeholder management, discussing roadmaps, milestones etc.	Up to 2 meetings with the Customer
Phase 2: Planning and Discovery	Assessment of the BYOD Environment Assessment of AD, AAD Planning (Project scope/eligibility/timeline/deployment) Reporting	Up to 2 workshops with the Customer One Solution Design Document
Phase 3: Design, Knowledge Transfer and Documentation	Service Design post assessment of BYOD Support system documentation gathering (system architecture/operation model/scripts) Decision making process (new application onboarding process/bug fix/Change request/release management) Knowledge transfer sign-off	Customer provided: (i) Knowledge articles, (ii) Operations/Support document. One Service Design Document
Phase 4: Service Establishment And Pilot	**Service Establishment (setup):** (a) Mobile Access Management (b) Mobile Security Management (c) ITSM Onboarding (if not done already) **Pilot setup:** (d) Service Readiness and Testing (e) Test case implementation (f) Acceptance Criteria	**Service Establishment Outcome:** Service Documentation including Policy, Configuration, Setup instructions. **Pilot Outcome:** (a) Test Results (b) Survey results (c) UAT feedback

Phase 5: Operate	Service Transition Sign-off and Go-Live. Interactive will move all Services into production and advise the Customer of the Service Start Date.	Transition Sign-off & Support documents

19.10 **Service Exclusions:**

The following exclusions apply to the BYOD Services:

(a) Hardware Break/Fix

(b) Hardware Support

(c) Lifecycle management of hardware, OS and software

(d) Device procurement and device disposal

(e) Device Encryption

(f) Any OEM/Vendor Support

19.11 **In-Scope Applications:**

(a) Interactive will provide the in-scope support as agreed with the Customer for the Applications listed in item (iv) below.

(b) Support for Applications is limited to accessibility and availability of the application on supported OS.

(c) Managed Applications are those that are supported by Microsoft Intune.

(d) In-Scope Applications:

Product Family	In-Scope Applications
Microsoft Office	Word, Excel, PowerPoint, Visio, Project, SharePoint, OneDrive, OneNote
Internet Browsers	Google Chrome, Microsoft Edge
Collaboration	Microsoft teams
Mobile Apps	Microsoft OneDrive and Microsoft Teams

20. Service Specification – Managed End User Device Services for Azure Virtual Desktop ("AVD")

20.1 If the CMS SOW states that the Customer has purchased Azure Virtual Desktop ("**AVD**") Services, Interactive will provide the following as further described in this Service Specification:

(a) Project Transition for AVD Services.

(b) AVD Host Pool Management.

(c) AVD Multi-Session Desktop Users.

(d) AVD Persistent Desktop Users.

(e) AVD Workstation Agent Health.

(f) AVD Patch Management Services.

(g) AVD Image Management Services.

(h) AVD Support for End Users.

(i) Microsoft Intune Platform Management.

(j) Application Packaging and Deployment Services.

20.2 Project Transition for AVD Management

(a) Clause 5.1 does not apply to the Managed End User Device Services for AVD, instead the following phases of the Transition Project apply:

Transition Service	Description	Outcome
Phase 1: Transition Kick-off	Introduction meetings, expectation setting, stakeholder management, discussing roadmaps, milestones etc.	Up to 2 meetings with the Customer
Phase 2: Planning and Discovery	Assessment of Azure Virtual Desktop Environment Assessment of AD, AAD, AAD Identity Protection, Microsoft Cloud App Security and Azure Advanced Threat Protection. Planning (Project scope/eligibility/timeline/deployment) Reporting	Up to 2 workshops with the Customer One Solution Design Document
Phase 3: Design, Knowledge Transfer and Documentation	Service Design post assessment of AVD platform Support system documentation gathering (system architecture/operation model/scripts) Decision making process (new application onboarding process/bug fix/Change request/release management) Knowledge transfer sign-off	Customer provided: (i) Knowledge articles, (ii) Operations/Support document. One Service Design Document
Phase 4: Service Establishment And Pilot	**Service Establishment (setup):** (a) Ticket Management Setup (b) Platform Readiness with knowledge share (c) Finalize ITIL practices (d) Configuration Management (e) Assignment of virtual desktops including resources required for monitoring configuration into AVD platform (f) Intune Setup and configuration (g) Setup Security Configuration and Policies for Endpoints (h) Application Packaging and Deployment (i) Application Hosting (j) Desktop Management using Intune **Pilot setup:** (a) Service Readiness and Testing (b) Test case implementation (c) Acceptance Criteria	**Service Establishment Outcome:** Service Documentation including Policy, Configuration, Setup instructions. **Pilot Outcome:** (a) Test Results (b) Survey results (c) UAT feedback
Phase 5: Operate	Service Transition Sign-off and Go-Live. Interactive will move all Services into production and advise the Customer of the Service Start Date.	Transition Sign-off & Support documents

20.3 AVD Host Pool Management

Interactive will provide monitoring and management of the AVD management platform and Host Pools, which consists of the following:

(a) Maintaining the AVD environment's pre-configured Azure Active Directory ("**AAD**") and Azure MFA integrations required for AVD operations.

(b) AVD platform management, alerting, investigation, and resolution.

(c) Monthly reporting and analytics regarding AVD platform alerts and tickets.

(d) Scaling the AVD platform up and down to accommodate planned User load changes.

(e) Modify AVD platform configuration settings.

(f) Alerting of PaaS management environment for critical events

(g) Investigate and resolve incidents relating to the AVD management platform.

20.4 AVD Multi-Session Desktop Users

Interactive will provide support, monitoring, and maintenance of the AVD multi-session desktop User service element, which consists of:

(a) Multi-Session User Desktop Host Management, alerting and resolution.

(b) Virtual Desktop Host availability monitoring (predicated on monitoring the primary host and not all hosts within the pool).

(c) Investigate and resolve incidents relating to the AVD Multi-Session Desktop Host and Pools.

20.5 Service Specification – AVD Persistent Desktop Users

Interactive will provide support, monitoring, and maintenance for the AVD persistent Desktop Users which consists of:

(a) Persistent Desktop User Host Management, alerting and resolution.

(b) Storage reporting for incident triage.

(c) Investigate and resolve incidents relating to the AVD Persistent Desktop Host and Pools.

20.6 AVD Workstation Agent Health

Interactive will provide services that ensures the functionality of the workstation Intune agent and Windows Updates agent which consists of the following:

(a) Software deployments.

(b) Windows update deployments.

(c) Anti-malware Endpoint Protection.

20.7 Remediation activities for systemic (system issue impacting multiple desktops) deployment issues such as:

(a) Remote resolution of agent health issues.

(b) Remediation of agent functionality to communicate with management system, send inventory and status updates.

(c) Agent upgrades

20.8 Workstation Agent Health Compliance Report: Interactive will provide a compliance summary report once every month.

20.9 AVD Patch Management

(a) Interactive will provide patching services for the AVD infrastructure which refers to the process of applying updates and security patches to the operating system, and core/supported Applications set out in clause 20.19 within the Customer's virtual desktop environment.

(b) Application Patching: Interactive will provide updates to the Applications installed on the Customer's virtual desktops which consist of the following:

(i) Applying Application-specific updates and security patches.

(ii) Reviewing the patch request.

(iii) Defining a delivery date within objectives

(iv) Identification of internal and external Application Package dependencies.

(v) Industry best practice Application Package creation.

(vi) Installation and removal process for each Application Package.

(vii) Deployment testing in a virtual test environment.

(viii) Packaging of pre-requisite software items for the packaging request.

(c) Patching Policies and Schedules: Interactive will provide patching policies and schedules to automate the deployment of updates. Interactive will help to configure maintenance windows during which updates are applied to minimise disruption to Users.

(d) Testing and Validation: Interactive will perform testing and validation in a non-production environment, based upon Customer having a non-production environment available, before deploying patches and updates to the Customer's production virtual desktop environment. This helps identify any compatibility issues or conflicts that may arise from the patching process.

(e) Reporting: Interactive will provide monthly reports on patching to the Customer. The effort to produce the reports will not exceed more than one hour per month.

(f) The table below sets out the high-level responsibilities between the Customer and Interactive for Patching:

Task	Interactive	Customer
Troubleshoot issues related to patching	R, A, C	I
Approval for patch maintenance window	C, I	R, A
Schedule patching	R, A	C, I
Business application verification, maintenance, and testing	C, I	R, A
Patch Deployment	R, A, C	I
Defining standard recurring deployment schedules, exclusions, and targets	C, I	R, A
Compliance measurement for SLA purposes	R, A, C	I
Add and remove systems to scope	R, A	C, I
Review released list of patches from Microsoft and provide customer notification prior to scheduled installation	R, A	C, I
Identify patches to be excluded and approve list of patches for deployment	C, I	R, A
Identify business areas that require patch reporting and provide contact information for recipients	C, I	R, A
Provide remediation for failed deployments due to patching	R, A, C	I
Run and provide reports per the agreed schedule	R, A, C	I

R=Responsible, A=Accountable, Consulted, I=Informed

20.10 AVD Image Management Services

(a) Interactive will provide the below set of image management services for operating systems of the Customer's AVD environments:

(i) Either create a golden image or base image that is regularly updated with the latest patches and updates OR create images using Azure templates and maintain them.

(ii) Maintaining the lifecycle of image.

(iii) Addition and deletion of applications within the image.

(iv) OS and software updates.

(v) Maintenance of task sequences.

(vi) Testing and validation of task sequences.

(vii) Remediation of failures related to task sequences.

(viii) Troubleshooting for image deployment failures.

(ix) Creating driver packages.

(x) Distribution of drivers within images.

(xi) Updating task sequence with drivers and driver packages.

(xii) Driver package testing.

(b) When provisioning new virtual desktops, the Customer can use these patched images to ensure that the desktops are already up to date.

20.11 AVD Support for Users

Interactive will provide below support to the Customer's Users:

(a) AVD client deployment: Interactive will create "How to" guides for the Customer's Users to self-deploy AVD clients on their individual desktops or thin clients. These guides will contain detailed instructions on setting up access to the AVD.

(b) Network troubleshooting: Interactive will provide support for network troubleshooting restricted to managed Devices only. This includes connection to Wi-Fi, host sessions and published Applications.

(c) RemoteApp: Interactive will provide Customer applications (installed on session hosts), that are published as RemoteApp.

(d) AVD Security: Interactive will provide support for password resets, MFA, conditional access (setup only), AD group (create the groups, management of users).

(e) Printing support: Support includes redirect print queues only (for local printers), User level support (How-To guides).

(f) Interactive will provide AVD support service that includes assignment of the virtual desktops including resources required for monitoring configuration into the AVD platform.

(g) Day-to-day monitoring and trend analysis may require additional resources be deployed on demand.

(h) More complex activities such as disruptive upgrades, migrations, template development, template deployment and projects are excluded but may be submitted as change requests and delivered by Interactive project services at an additional charge.

20.12 Microsoft Intune Platform Management

Interactive will provide the below services as part of Intune Platform Management, unless it is already provided under Managed End User Device Services:

(a) Administration

(i) Intune platform administration and monitoring.

(ii) Autopilot Administration.

(b) Remediation of issues with Intune.

20.13 Interactive will configure and set up Intune unless it has already done so during the Project Transition phase for the Managed End User Device Services.

20.14 Application Packaging and Deployment

(a) Interactive will provide the following Application Packaging and Deployment Services for standard and Simple Applications only (i.e., .MSI and .exe), up to 10 Applications for AVD scope, unless it is already provided under Managed End User Device Services:

(i) Review the Application for packaging request (e.g. Win32 or MSI).

(ii) Identification of all dependencies for the Application Package.

(iii) Installation and removal process for each Application Package.

(iv) Deployment testing (test environment).

(v) Identification of Rings for Deployment.

(vi) Reporting.

(b) Interactive will support Application Packaging and Deployment of In-Scope and Simple Applications, up to 5 new Applications per month. Any additional Applications will be charged based on standard rate card.

20.15 Pricing:

This clause applies in place of clause 9 for the AVD Services only:

(a) The monthly Service Fee for Managed End User Device Services for AVD is calculated based upon the agreed number of Persistent Users and Pooled Users as set out in clause 2 of the CMS SOW. If the Customer adds any new Persistent Users and Pooled Users, standard rates from the service catalogue will apply.

(b) Monthly Service Fees for Managed End User Device Services for AVD are payable by the Customer from the Service Start Date. Interactive will issue invoices to the Customer for these AVD Services.

(c) Interactive may adjust the Service Fee annually for each of the Services detailed in the CMS SOW (for the avoidance of doubt, this change applies to both initial and additional Services) by giving no less than 30 days' notice to the Customer.

(d) Interactive may vary the monthly Service Fee when a variation to the Services is necessary due to Changes in the number of Users, and this shall occur as either an addendum to the CMS SOW or in accordance with the Change Management process.

(e) Any Application Packaging request over the agreed number of Applications (as specified in this Service Description) will attract an additional Service Fee per Application will be charged in accordance with the Standard Charge Out Rates.

20.16 Customer Responsibilities:

(a) The Customer must have subscription for Azure and may either:

(i) Purchase the subscription from Interactive under a separate Statement of Work, in which case Interactive will provide Azure Platform Support; or with Interactive as pre-requisites to this service.; or

(ii) directly from Microsoft, in which case Interactive will not provide Azure Platform Support. Interactive will only provide the Setup of the Azure Platform required for ongoing management of Managed End User Device Services for AVD.

20.17 Service Exclusions:

The following exclusions apply to Managed End User Device for AVD Services:

(a) **AVD Multi-Session Desktop Users**

(i) Resolution of connectivity and Customer issues outside of the AVD platform scope (e.g., internet / Customer WAN connectivity and performance, Application servers hosted on-premises being targeted by the Customer applications, etc.

(b) **AVD Persistent Desktop Users**

(i) Resolution of connectivity and Customer issues outside of the AVD platform scope (e.g., internet / Customer WAN connectivity and performance, application servers hosted on-premises being targeted by the Customer applications, etc.

(c) **AVD Patch Management Services**

Service exclusions for OS Patching:

(i) Development of patch "workarounds" in the absence of an approved system vendor's patch.

(ii) Ad-hoc and/or custom reporting.

(iii) Manual patching of systems.

(iv) Removal of patches from systems once installed.

(v) The use of 3rd party application vulnerability scanning, patching and remediation tools.

(vi) Performing manual vulnerability remediation steps.

Service exclusions for Application Patching:

(i) Packaging Software licenses for products like InstallShield.

(ii) Support for application packages, deployments and software not deployed.

(iii) Licenses for software being deployed.

(iv) Interactive login to workstations.

(v) Ad-hoc and customer deployment status reporting.

(vi) Manual installation of Application Packages.

(vii) Removal of Applications installed using any non-standard method.

(d) AVD Image Management Services

(i) Feature updates.

(ii) OS hardening.

(iii) Changes to hardware model.

(iv) Driver maintenance and updates.

(e) AVD Support for End Users

(i) Interactive will not provide any backup and restore of data stored on M365 apps such as SharePoint. The Customer must purchase additional product (Metallic/Cloud Protection) from Interactive if they wish to receive similar backup services.

(ii) Interactive will not be liable to perform any hardware maintenance, repair, or support for Customer's User Devices.

(iii) Cyber Services such as MDR, unless the Customer has purchased it as a separate product from Interactive.

(iv) Interactive will not provide any device lifecycle management for Customer's User Devices. This includes device refreshes, device refurbishing, Device upgrade etc.

(v) Interactive will not be able to support any User self-service capability on AVD. If the Customer wants to leverage such capabilities, they can do so by investing in third party products (e.g., Nerdio Manager).

(vi) Interactive may choose to leverage Industry-leader third party MSP managers such as Nerdio to help partners easily estimate costs and automate, manage, and optimize Windows Virtual Desktop deployments.

(vii) Management of physical desktop hardware issued and used by the Customer's employees, which is usually delivered via a traditional Managed End User Device Services.

(viii) Deployed applications are not supported except for the issue of AVD service availability and deployment issues. Application support remains with the existing Customer application support teams.

(ix) Desktop Management does not include management of mobile devices (e.g. iPhone and Android devices). Desktop remediation does not cover user support, and the scope is restricted to cover systemic agent health problems.

(f) Application Packaging and Deployment

(i) The Customer will perform all Application compatibility testing for any new Application Package request.

(ii) The Customer must:

A. Provide Interactive with all necessary Vendor Application sources.

B. Provide Interactive with Application Packaging requirements and instructions.

C. Provide the staging and testing environment.

D. Perform all functional testing of new Application Packages.

E. Provide Interactive with the User Acceptance Test (UAT) Plan.

F. Perform UAT testing and Application Packaging sign off to enable Interactive to deploy into production.

(g) General

(i) The management of User Devices is delivered via the Managed End User Device Services. This service does not cover the management of physical desktop hardware, mobile devices (smartphones/tablets) that are issued and used by the Users.

(ii) This service does not offer support for the User Devices.

(iii) No support would be provided for any deployed Applications, except if the issues caused are related to accessibility, availability or deployments associated with AVD services.

20.18 The following are Customer Dependencies:

(a) License requirements:

(i) The Customer is responsible for having the appropriate licenses for AVD usage, AVD is part of M365 licensing which can be sold by Interactive if required.

(ii) The Customer is required to comply with the license requirements set out on the Microsoft website: as below: https://learn.microsoft.com/en-us/azure/virtual-desktop/prerequisites?tabs=portal#operating-systems-and-licenses

(b) The Customer is required to have the following in place:

(i) Microsoft 365 or Windows 10 /Windows 11 Enterprise licensing.

(ii) On-premises Active Directory identity extended into Azure AD.

(iii) A Microsoft Azure subscription.

(iv) Interactive's AVD Platform Support.

(c) Application Packaging and Deployment assumes the following pre-requisites when using Microsoft Intune:

(i) Latest release of Windows 10 Current Branch.

(ii) 8 GB maximum size per application when using Microsoft Intune.

20.19 **In-Scope Applications**

(a) Interactive will provide the in-scope support as agreed with the Customer for the Applications listed in item 20.19(c) below.

(b) Support for Applications is limited to accessibility and availability of the Application on supported OS.

(c) Managed Applications are those that are supported by Microsoft Intune.

(d) In-Scope Applications:

Product Family	In-Scope Applications
Microsoft Office	Word, Excel, PowerPoint, Visio, Project, SharePoint, OneDrive, OneNote
Internet Browsers	Google Chrome, Microsoft Edge
Collaboration	Microsoft teams
Mobile Apps	Microsoft OneDrive and Microsoft Teams

21. Definitions

21.1 Unless the context otherwise requires, words and expressions defined in the Master Services Agreement have the same meaning in these Terms and any terms not defined herein have the meaning set out in the Master Services Agreement.

21.2 The following definitions of terms apply to the Managed End User Device Services – Service Description:

Active Directory (AD) means the database and set of services that connect users with the network resources to enable them to perform work. The database (or directory) contains critical information about the Customer's environment, including what users and computers there are and permitted functions.

Azure Active Directory ("AAD") is Microsoft's multi-tenant, cloud-based directory, and identity management service. It is an enterprise identity service that provides single sign-on, multifactor authentication, and conditional access to guard against 99.9 percent of cybersecurity attacks.

Application Packaging Services means the process of bundling application source files and software components and configuration settings into a single application bundle (package) which can be distributed and installed without user or administrator interaction. Packaging of applications provides a repeatable standard installation of applications where all installation options are predefined and determined as part of the packaging process thus providing a common look and feel for the application across many users.

Asset Register refers to the list of Devices used by the Customer's End Users. This list is provided by the Customer to Interactive that would be updated in the MDM Tool by Interactive.

AVD Persistent Desktop infrastructure is a setup in which each User owns a virtual desktop whose settings and customizations are available to the User each time they log in.

Azure Virtual Desktop is an application and desktop virtualization service the Customer can use to access Windows Applications and desktops from anywhere, using any device.

Bring Your Own Device ("BYOD") means a Users' laptop, tablet or mobile phone that is owned by the Customer's User or other third party that is not the Customer.

Change means the addition, modification, or removal of anything that has, or could have, an effect on the IT Environment.

Devices means the Customer owned and supplied desktops, laptops, mobile phones, tablets, thin clients that have been onboarded to the Managed End User Device Services.

EUS stands for End User Support for the Customer Device related issues.

IT Environment means the Customer's IT environment, including applications, networks, servers, hosts and workstations, which may be located or hosted at the Customer's premises or hosted externally (for example, at an Interactive facility).

IMAC means, for Devices, installation, moves, adds or Changes.

Jailbroken or Rooted means the process of bypassing software restrictions put into place by the device manufacturer. Jailbroken is mostly associated with Apple devices, whereas, rooted is linked to Android devices.

Level 3 Support means Escalated support for issues that could not be fixed by Level 1 and Level 2 Service Desk teams.

Level 1 and Level 2 Support refers to basic troubleshooting and support offered typically by a Service Desk team. This may involve teams from Interactive or the Customer side**.**

Managed End User Device Services means the services described in this Service Description.

MDM tool refers to Mobile Device Management tool that is used to enrol, configure and govern user devices such as desktops, laptops, smartphones, tablets, thin clients in a customer's environment.

Mobile Devices refers to smartphones, tablets (iOS and Android).

Master Image refers to OEM-optimized image of Windows 10/ Windows 11 provisioned using Microsoft Autopilot. This version is preinstalled on the device, so one doesn't have to maintain custom images and drivers for every device model**.**

MOE means the managed operating environment maintained by Interactive in accordance with the Service Specification for MOE Management.

Onsite Location means the Customer's locations as specified in the CMS SOW, where onsite Managed End User Device Services will be performed.

Remote Location means the Customer's locations as specified in the CMS SOW, for which Managed End User Device Services will be provided remotely (which may be from any Interactive or contractor location).

Persistent User are AVD Users who are allocated a dedicated desktop.

Pooled User are AVD Users who are allocated to whichever session host is currently available.

Priority means the product of the Impact and Urgency as defined via the matrix in item 19.9 of the Managed End User Device Service Descriptions.

Software Distribution consists of automated remote distribution of software on client machines leveraging existing network infrastructure.

Tenant is a reserved Azure AD service instance that an organization receives and owns once it signs up for a Microsoft cloud service such as Azure, Microsoft Intune, or Microsoft 365. Each tenant represents an organization and is distinct and separate from other Azure AD tenants.

Third-Party Fault means where the root cause is solely or partly the responsibility of a third-party (such as a telecommunications provider or Customer contractor).

Third-Party Software means programs or applications created by companies other than Interactive, which Interactive provides or licenses to the Customer in accordance with this Statement of Work, which includes but is not limited to the Customer Portal.

Third-Party Software Vendor means a company that creates Third-Party Software or supplies Third-Party Software to Interactive.

Telephone and Expense Management (TEM) provider means the telecom network provider such as Telstra, Vodafone etc providing mobile network services to the Customer.

Update means a minor release of the same version and does not include upgrades to major versions.

Users means the Customer's employees or contractors that are set up as users in the Customer's Active Directory and under the scope of Digital Workplace support by Interactive.